
Password Agent

User's Manual

Rev 2.6.1

Contents

Introduction	4
Description.....	4
Lite vs. Unlimited	5
Privacy	5
How secure?	6
Security scheme	7
 Tutorial	 9
Creating a new file & setting master password.....	9
Program layout.....	11
Groups	12
Adding a group.....	12
Renaming a group	12
Deleting a group	12
Moving a group	13
Changing group color	13
Entries.....	13
Adding an account entry.....	14
Adding a note entry	14
Editing an entry	14
Deleting an entry	14
Moving an entry	15
Entry Properties window	15
Saving your file.....	17
Undo feature	17
Opening a file	17
Security features	18
Locking a file.....	20
Searching	20
Using QuickSearch.....	20
Using the Find tool.....	21
Printing	22
Sorting	23
Hiding and reordering columns	23
Useful tools & functions.....	24
Password Generator	24
Options.....	25
Main tab.....	25
Colors tab	28

Templates tab	29
Hot keys tab.....	29
Common User IDs tab	29
Multiple users	29
Tips & tricks	29
Advanced Features	30
Automatically filling login prompts.....	30
Autofill using global shortcut key	31
Basic autofill.....	31
Sample workflow using autofill	32
Templates.....	32
Taking the program with you.....	33
TakeWithMe wizard.....	33
Running Password Agent from removable disk	34
Using expiration date.....	35
Command Line	35
Import & export.....	36
Import.....	36
Export.....	36
Keyboard shortcuts	37
Network installation.....	37
Solving problems	38
Autofill feature does not work	38
Autofill enters double/invalid password	39
Global hot key does not work	40
Open Link command does not open web pages.....	40
Web links open in the same browser window.....	40
Slow or erratic scrolling in entries list	41
File is damaged.....	41
Administrator privileges required.....	41
Knowledge base & forum	42
How to buy	42
How to Buy.....	42
Entering a key code	42
Uninstalling & Contact Info	43
Uninstalling Password Agent.....	43
Contact information	44
Credits.....	44
Index	45

Introduction

Description

Password Agent is a powerful yet compact and easy to use password manager program that allows you to store all your passwords and data snippets in a single, easy to navigate and secure database. It is not limited to storing only passwords – you can store any information you want, like key codes and serial number of purchased software programs, bank account numbers, credit card numbers, membership numbers, magazine/newspaper subscription dates etc. Storing all your useful information in one place makes it very easy to find it when required and you can also backup all this data at once just by copying single database file.

Main features:

- Fast, compact and easy to use program with familiar interface similar to *Windows Explorer*.
- Encrypted password database files, accessible only via user selectable master password (for enhanced security, master password is used as encryption/decryption key only and is not stored anywhere). You can also assign a short master password hint text so if you accidentally forget your master password, the hint will help you to recall it.
- Unlock window where you enter master password contains function to confuse key loggers, so if any key loggers are present in the system where you enter master password, your password will not be logged by key logger in plain text but is mixed with randomly generated additional keystrokes.
- Make custom groups/subgroups to divide your entries into logical groups for easier access.
- Each account entry consists of Title, UserID, Password, Link, Note, Date Added, Date Modified, Date Expire and Old Password fields. You can also make Note entries that do not have UserID and Password fields. All text fields allow virtually unlimited length of text, so you can store long memos in Note field.
- Option to close or lock the program automatically after defined period of inactivity or when screensaver starts. So the program will lock automatically if you are away from your computer.
- Fill login prompts with required data (customizable per entry by template), thus reduce typing.

- Includes password generator that generates unique non-guessable passwords.
- Powerful *QuickSearch* function that allows you to easily filter and display entries across all groups.
- Print hard copy of your database.
- Export your database to HTML (grouped or columnar), XML or CSV. Import entries from other password database programs in CSV format.
- Custom sorting and column order.
- View/hide sensitive information switch, you can mark what columns contain sensitive information.
- Multiple users can open the same password database file over network or as different users on the same computer (first user have full read/save access, other users will have read-only access).
- Strong U.S. government approved AES encryption with 256-bit key.
- Compact files - its password database file that contains 100 entries may be below 10 kilobytes in size!

Lite vs. Unlimited

The *Lite* version is free but allows you to store up to 25 entries per file. If you need to store more entries, you may purchase the *Unlimited* version. The *Unlimited* version can store virtually an unlimited number of entries. There are no other differences between *Lite* and *Unlimited* versions.

If you have just purchased the *Unlimited* version, see “Entering a key code” on page 42.

Privacy

We guarantee that none of our software has built-in functions that can contact us without your knowledge or send any of your information to us without your knowledge. Some our programs have *Check for Update* functionality that can be used to check if there is a new version of the program available. This function is fully manual, so it is used only if you invoke this command manually. During update checking the program will open a new web browser window that sends name of the program, major, minor and build numbers to our server. No personal information is transferred, including your name, serial number etc. Programs never contact our server directly, but open your default web browser to establish connection and display result.

Warning: Be careful when using the program in public computers (at work, internet cafes etc). Using special logging and spy software it is possible to log all computer activity, including your master password and other data you enter or view on screen. If such program is installed then someone can steal your master password and other data you enter through *Password Agent*. This is true for all Windows applications, not only for *Password Agent*. For example it is possible to log all passwords you enter manually into your web browser or all text you enter using keyboard; all active programs, mouse clicks etc. See “How secure?” on page 6 for more information.

How secure?

People often ask, how secure is *Password Agent*. Is it 100% secure? Even when the data file is encrypted using one of the best “strong” encryption algorithms, there are several other factors that endanger total security. And unfortunately these others factors are often overlooked, making people think that total security depends on the “key length” that is used to encrypt you data.

Assume there is someone who is planning to get access to secrets you are keeping in *Password Agent*. You need to know that there are several ways someone may try use to get access to your secrets, so lets analyze them and make some conclusions.

Stealing your data file

If someone will get access to your data file, don’t worry. He will not get access to the secrets if he doesn’t know your master password. It is very unlikely someone is able to decrypt the file without valid master password using today’s computers. But as today’s best encryption methods are considered “strong”, something may happen tomorrow that will make them obsolete instantly. This is unlikely, but still possible.

Risk – very low.

Dumping memory

Another potential way to steal your info is to use special Trojan program to dump *Password Agent*’s memory to a disk file, then later try to find any plain text info from this file. To prevent this, *Password Agent* keeps data in memory in scrambled form. It is unlikely something will leak that way, but possible (see “Security scheme” on page 7). **Risk – low.**

Swap file

Windows manages a swap file – it is memory extension on hard disk, called virtual memory or page file. Since programs and data files may be very large nowadays, everything can’t be kept in limited computer memory at the same time, so Windows now and then writes data and running programs not used at the moment from RAM to hard disk. That means on one moment *Password Agent* and any other program may end up written to swap file along with all memory in use and there is no way to prevent this. That is almost identical to our previous “Dumping memory” case, but done regularly by Windows itself! If you are on a public computer then someone can potentially try to search the swap file for plain text, but *Password Agent* keeps data in memory in scrambled form, that makes this difficult (see “Security scheme” on page 7). Swap file can be only accessed when Windows is shut down. **Risk – medium.**

Social engineering

That is old truth and known to everybody – the simpler the password the easier is to guess it. Don’t use simple master password. Don’t use your name, your dog’s name, your wife’s name, your children’s name, your favorite actor name, any of your favorite things, known dates etc as your master password. If someone is trying to get access to your secrets, that is what he will try first. Use something much more abstract, like several random words combined with some numbers or even better, totally random string. **Risk – high.**

Spy programs

There are too many spy programs available that allow someone to secretly watch and record your every key press, including your master password you type, text you copy to clipboard, screen captures, mouse movement and clicks etc. Basically everything you see on the screen can be also recorded, so on public computers is impossible to

warrant secure work environment. Although from version 2.6 *Password Agent* contains function to confuse key loggers during entering master password, using the program in public computers is not recommended if you data files contain any secret information. The same applies to other people's computers that are out of your control. **Risk – very high.**

Conclusions?

As you can see, final security depends mostly on other factors than encryption algorithm and key length used. Your file may be encrypted using the best encryption available, but if someone can easily just “steal” your master password using key logger or social engineering, then even the best encryption will not help.

To make long story short – total security depends also on you.

Note: On Windows NT/2000/XP/Vista/7 it is possible to tell Windows to clear swap file on shutdown. You can do this by selecting **Clear page file at shutdown** option (see Security options on page 26). This will reduce the risk that something will leak through the swap file, but if computer crashes or is switched off without normal shutdown procedure, this procedure will not be carried out, leaving the swap file as is. If this option is active, Windows shutdown process will take much more time because the swap file will be overwritten.

Security scheme

Note: This topic is for advanced users.

This topic discusses how exactly *Password Agent* works behind the scenes, what kind of encryption is used in *Password Agent* and also some possible weak points of the program that may potentially leak your information. You can then decide if this kind of security is enough for you or not.

Encrypted data files

Data files on the disk, where the data is stored (*.PWA files), are encrypted with strong AES (Rijndael) algorithm using 256-bit key that is created using Haval algorithm from user's master password. Rijndael was chosen lately as new U.S. government encryption standard to replace older DES and is now called AES (Advanced Encryption Standard):

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

All data stored in disk file is encrypted, except master password hint (if provided).

Master password

The master password itself is not saved in the disk file. Instead, its hash is stored in encrypted form. When user wants to open a data file, he is asked to enter master password. *Password Agent* will then make a hash from entered master password, and will decrypt part of the disk file where the actual hash is stored. Then these two hashes will be compared and if they are the same, valid master password is provided by user. The actual master password is not kept in memory or anywhere, only its hash.

Data in memory

Keeping data in memory as safe as possible is also part of program's design - something that is very often overlooked and many password managers don't pay

attention to this, putting your secret data in danger. We need to do this to prevent our secrets end up plain text in swap file or to prevent someone from stealing our secrets by dumping *Password Agent* memory into a disk file.

For performance reasons, *Password Agent* keeps memory data scrambled using simpler, reversible ‘pseudo-key’ algorithm (XOR-like, but much improved), not the same strong encryption algorithm AES that is used for data files. Encryption key for memory data is a random string that is different each session.

Data fields that are scrambled in memory: Title, UserID, Password, Link, Template and Note. Group names are not scrambled and are kept in plain text format.

Possible plain text leaks

First, these plain text leaks are issue only in non-controlled/public environment, where very high security is needed. Plain text leak means that some of your secret data may potentially end up in Windows swap file or RAM and when someone specialist is specially looking for it, he may find it. It does not mean that *Password Agent* will leave temporary files or text files on your disk, readable by anyone.

Normal *Password Agent* operation, including autofill functionality, should not leak any plain text into memory or swap file.

The number 1 plain text leak is when using clipboard functions. That means **Copy Password**, **Copy Note** and all other **Entry | Copy ...** functions. *Password Agent* will clear clipboard automatically, but nevertheless copied text may remain in global memory due to Windows design.

The following functions will leak plain text in big amounts: **Import CSV**, **Export HTML/XML**. These are not optimized to be safe due to their huge use of string tokens and rare usage, but this may change in the future. When using these import/export functions in an environment that requires very high security it is advised to restart computer after completion.

Finally, when *Password Agent* tries not to leave any plain text in the memory, we can’t take responsibility about all the other software where you send your secrets using autofill or by any other means.

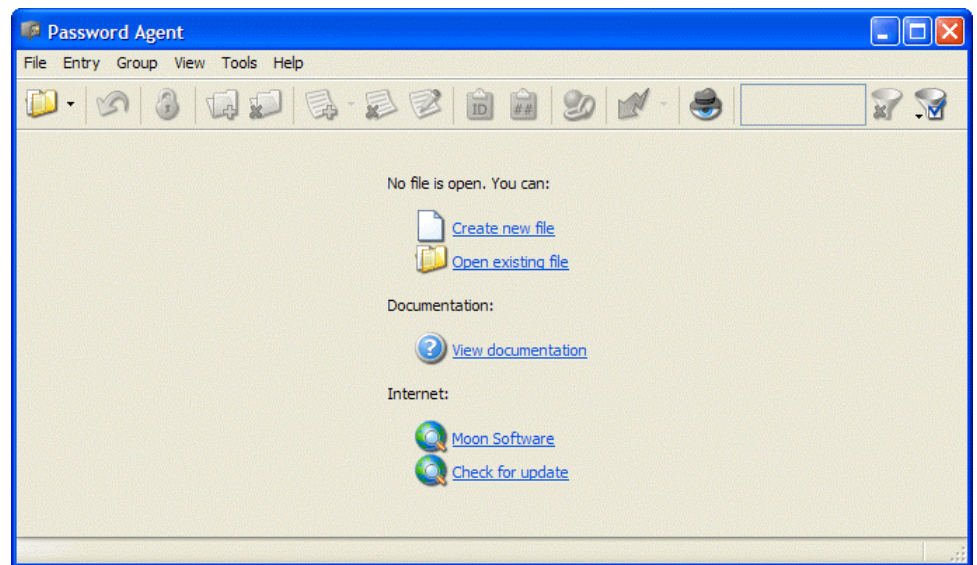
Backdoors

There are no backdoors in the program, so if you forget your master password, we can’t open your file. Master password is not stored anywhere, so there is no way to “retrieve” it. So be careful with your master password.

Tutorial

Creating a new file & setting master password

When you launch *Password Agent* for the first time, you'll see the following screen:

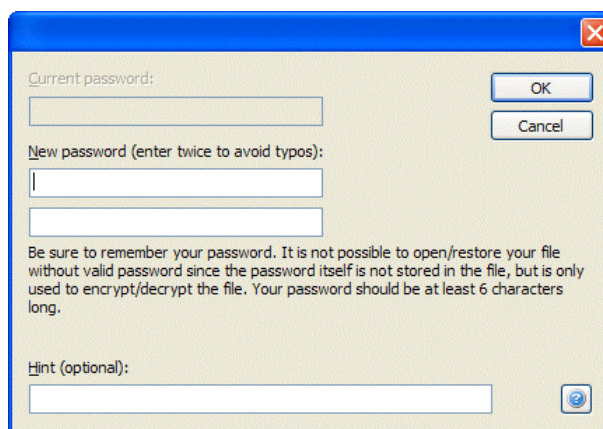


To start using the program, you'll need to create a database file where *Password Agent* can store your data.

If you are new to *Password Agent*, you'll need to create a new file (if not, see "Opening a file" topic):

1. Choose **Create a new file** link or **File | New** command from menu. A message is displayed that this is a 2-step process. Press **OK**.
2. Now *Save As* window is displayed, asking for file name. Type name for your password database file, it may be good idea to use your name (like "John") if there are more users for your computers besides you. You can select also different folder if you wish, but by default your file is saved under *My Documents* folder. All your data you enter into *Password Agent* will be saved into this disk file. After typing your file name, press **Save**.

3. *Master Password* window is displayed.



Every password database file must have master password specified. It is used to restrict access to the file, so only people who know the master password can open the file and see its contents. You are required to supply your master password every time you open your file.

Note: It is important to understand that master password is assigned to each file separately. Master password is not a password that allows you to get access to the *Password Agent* program, but *Password Agent* uses it to encrypt and decrypt the file contents. For example, if your friend brings his own *Password Agent* database file to your computer, then only his master password can open his file, not yours.

Choose a master password for your file and enter it in the *New Password* field (don't worry about the disabled *Current Password* field, it is not used this time). Try to choose a long, hard to guess password, since if anyone guesses your master password, they will have access to all your other passwords stored in the *Password Agent* database file too. Enter the same master password once again, into the next field. This is for making sure you did not make an error or "typo".

Warning: You should be very careful not to forget your master password, because if you forget it, no one, even us, can open the file.

Into the *Hint* field you can write something that will help you to recall the master password if you happen to forget it. You can display this password hint text when you need to enter your master password. Please note this text is visible to all people who are trying to open your encrypted file, so don't use something too simple that could help others to guess your password.

If you are finished typing your passwords, press **OK** to finally create the file.

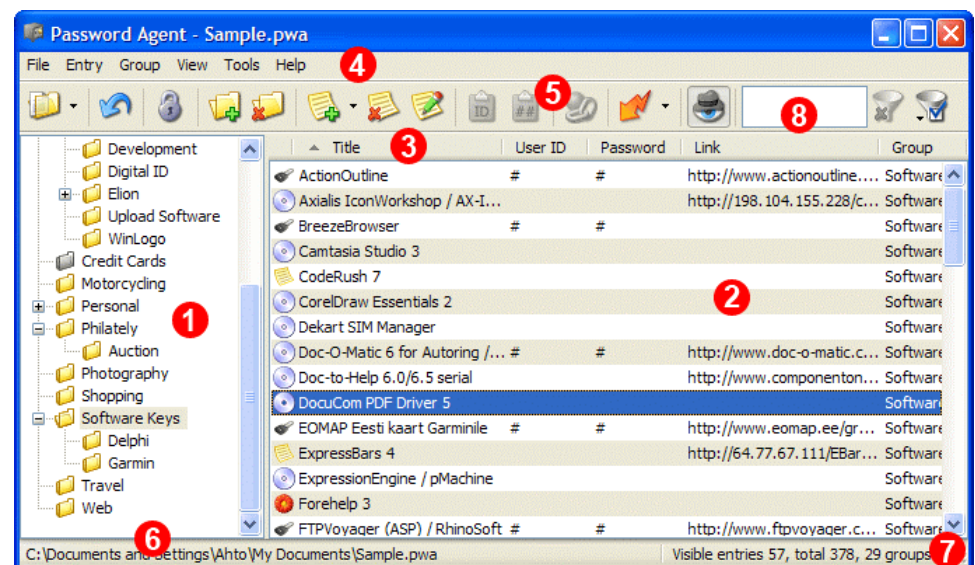
At this point *Password Agent* has finished creating your file and you can start entering your data. See the following topics about program layout and how to add your first entries.

Program layout

Password Agent has a simple 2-panel (left and right side) layout similar to *Windows Explorer*. On the left side you see a hierarchical tree that displays the groups. You can click groups with the mouse to display their contents in the right panel. Initially the left panel (lets call it the "groups tree" from now on) only lists one root entry titled "Root". The right panel, as mentioned, displays entries that the selected group contains (we will call it the "entries list" from now on).

Other parts of the program are menus, toolbar and status bar. You use the menu and toolbar as in other programs - there is nothing really different with them. Status bar displays info about state of the program, see image below for description of status bar sections.

The groups tree and entries list have right click (context) menus, so you can perform common actions just by right clicking on a group or entry. There are context-menus available for the entries list column headers and main toolbar as well.



Explanation of the main screen:

1. Groups tree. Right-click to display context-menu.
2. Entries list, displays entries from group selected on left tree. Right-click to display context-menu.
3. Header control of entries list. Press column title to sort by that column, drag with the mouse to rearrange columns. Right-click to display context menu.
4. Main menu bar.
5. Toolbar buttons for fast access to most used menu commands.
6. Name of currently open data file.
7. Count of currently visible entries (if group is selected or filter is active), total count of entries and count of groups.
8. QuickSearch text entry box allows you to quickly find an entry by typing part of its title.

Groups

You may create groups to keep related entries together. If you have many entries, this helps to navigate through your password entries faster. You don't need to create any groups at all to use *Password Agent*, but groups help you to organize your data better. You may find it helpful to think of groups in *Password Agent* as folders in your file system. You work with groups the same way as folders in a filing system.

Tip: You can perform most group-related commands also by right-clicking on a group. That will invoke context menu that displays the same commands that are in the **Groups** menu.

Adding a group

1. To create a new group, choose **Group | New** command. Note that there is now a new node visible in the groups tree, titled "*Untitled group*" and it is in edit mode.
2. Type in the name you want to use, and press the **Enter** key.

Each new group is created as a subgroup of the selected group. So, if you have a group selected and use the New group command, the new group is automatically created as a subgroup under the selected group. To create top-level groups, the virtual root group titled "Root" must be selected first.

Renaming a group

You can rename a group anytime you wish:

1. Select the group you want to rename
2. Press the **F2** key or choose **Group | Rename** command. The group node changes to edit mode.
3. Type in the new name, and press the **Enter** key. If you don't want to finish renaming for any reason, you may cancel editing by pressing the **Esc** key.

Deleting a group

To delete a group:

1. Select the group you want to delete.
2. Press either the **Delete** key, or use the **Groups | Delete** menu command. Alternately, you can use the mouse to highlight, and right click to bring up the groups menu.

If your group was empty, it will be deleted immediately. But if your group, or subgroup below it, contains entries, *Password Agent* will display "Delete group" window asking what you would like to do with the accounts the group contains. You may either keep the accounts by moving them to a group of your choice, or you can tell *Password Agent* to permanently delete those accounts.

Note: You cannot delete or rename the *Root* group. The *Root* group is a special built-in virtual group that represents all entries in database. Selecting this group will display all entries in the entries list, no matter into what user-defined group they belong. That way you can list all entries at the same time, even from different groups. Also, since it is possible to create new entries that do not belong to any user-defined group, *Root* group is the only way to list these entries since they only belong to that virtual group automatically (as do all other entries).

Moving a group

You can move a group by dragging it with the mouse. By dragging one group over another and then releasing mouse button will make the dragged group subgroup of the target.

To cancel already started drag operation, press the **Esc** key or drag the group outside the groups pane.

Changing group color

You can change color of a group image that is displayed in the group listing. That way you can mark certain groups to be different so you'll locate them more easily.

1. Select the group you want to change.
2. Choose **Group | Change Color** and choose a new color from the displayed submenu.

To restore the default yellow color, just repeat the process but choose the yellow color.

Entries

Password Agent allows you to use two different kind of entries – account and note entries.

An account is a small collection of information related to one object (web site/program/credit card etc). An account can consist of the following main fields: *Title*, *UserID*, *Password*, *Link*, and *Note*. You don't need to provide all the information, only the fields you want to store.

For example to access the Internet, your service provider usually gives you special user name and password so only authorized customers can connect their computer/server. We call this information *user account* (or just *account* for short). On the other hand, many web sites nowadays require you to register to create an account on their site, especially Internet stores. So you can easily create and store these accounts in *Password Agent*.

In addition to password accounts you can create special note entries. They are simple entries that can be used to store free form textual information, like your software serial numbers, credit card numbers, secret notes etc. Note entries are similar to account entries except they don't have *UserID*, *Password* and *OldPassword* fields, but simply use the *Note* field to store your information.

People are sometimes confused how they can store their credit card or other specific data when there is no special credit card entry type. The note entry allows you to store any kind of textual data, just don't think you are not allowed to type your data here because the name of the field is *Note*.

Adding an account entry

To create a new account entry:

1. Choose **Entry | New Account** command. The *New Account* window is displayed (see “Entry Properties window” topic for details).
2. Fill in the fields you need, and press **OK** button.

Your new entry should now be displayed in the entries list.

Tip: The data entry window is resizable so if it looks too small you can resize it to your taste by dragging its border with the mouse.

Adding a note entry

Creating a new note entry is identical to creating a new account entry (see previous section), except note entries don’t have *UserID* and *Password* fields.

1. Choose **Entry | New Note** command. The *New Note* window is displayed. See previous section “*Adding an account entry*” above about field descriptions.

Editing an entry

To edit an account or note entry:

1. Double-click it with the mouse, or select it and choose **Entry | Properties** command from the menu. The *Properties* window is displayed. Pressing the **Enter** key in entries list also displays the *Properties* window about selected entry.
2. Make the modifications you need, and press the **OK** button.

Deleting an entry

To delete an entry:

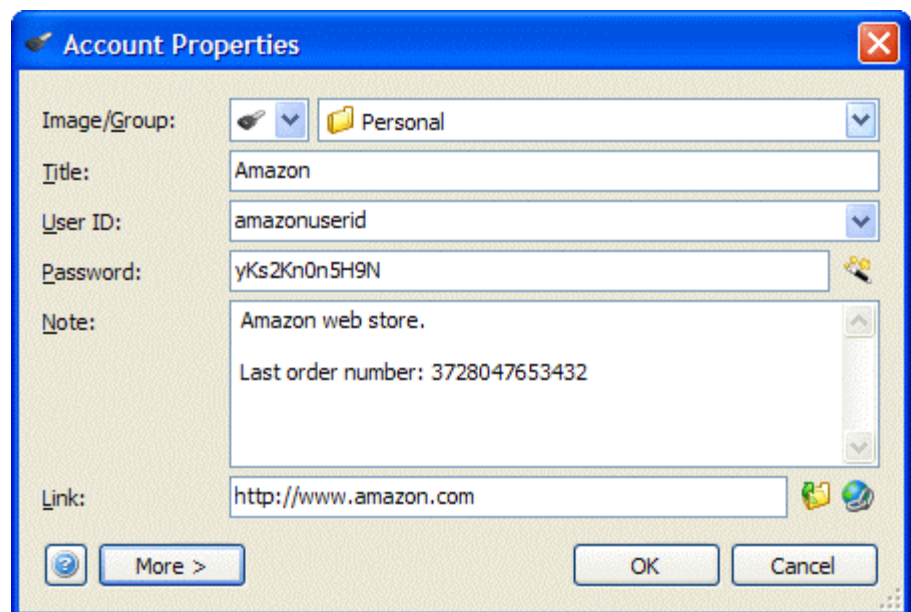
1. Select the entry you wish to delete by clicking it with the mouse.
2. Press the **Del** key, or choose **Entry | Delete** command.

Moving an entry

You can also move an entry from one group to another by dragging it with the mouse just like you can drag files in *Windows Explorer*. Alternatively you can just edit an entry and change its group in *Entry Properties* window.

Entry Properties window

After main window, this is the next frequently used window in *Password Agent*. It will be displayed when you create a new entry or edit an existing one. For note entries *UserID*, *Password* and *Old Passwords* files are not displayed.



Available fields are:

Image - You can choose a different image to represent this entry. By default, *Password Agent* chooses a key image for account entries and a note image for note entries. That way you can distinguish note entries from account entries in the entries listing. You can choose a different image to make certain entries stand out, but if you have no idea what to do with the image, leave it as it is.

Group – Choose a group where you want the new entry to belong to. If you don't have any groups, don't worry, you can easily change or add a group later. By default current group is selected.

Title - is the name you give to your entry. For example, if you want to add an entry containing your Amazon.com web site user name and password, you can title it "Amazon" or "Amazon.com" (without quotes). Be descriptive when naming your entries, since if you have hundreds of entries later, descriptive names will help you to find the right entry quickly.

UserID - this is user name/user ID field. This is actually a drop down box. You can add your most used user IDs to the drop down list for quick access and also configure the program to automatically fill this field when you create a new account

entry. See *Common User IDs* tab under *Options*. This field is displayed for account entries only.

Password - this is your companion password for your user name/user ID. If you have not been given a ready made password by a third party, you may pick your own password, or *Password Agent* can generate a password for you if you press the **Generate Password** button next to the *Password* field. This field is displayed for account entries only.

You probably noticed that when the *New Account* window was displayed, the *Password* was already filled in. By default *Password Agent* generates you a new password “in advance” using its built-in password generator. Of course you don’t need to use that password and can replace it with your own. You can turn off the automatic password generation feature under *Options*.

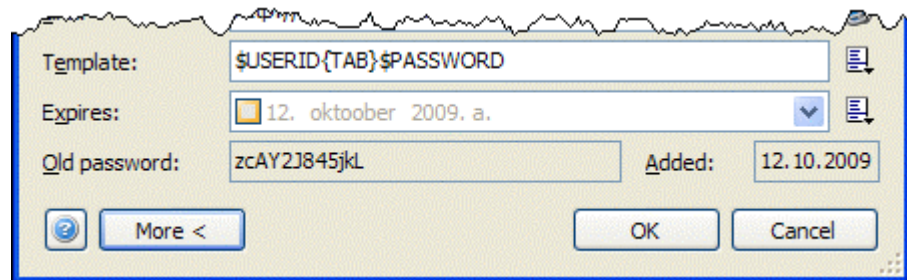
Link - this field is not required, but you may find it useful, especially if this entry is about a web site. For example, you can put the web link "http://www.amazon.com" here. If link is provided, *Password Agent* can launch it with the **Entry | Open Link** command. Also, you can put the full file name of a program executable here or another file, so you can run this external program/file using **Entry | Open Link** command.

Right after the *Link* field is **Browse link** button that you can use to browse the file or program from your file system. **Test link**, the second button after the *Link* field can be used to execute the link -- to test if that is working as expected.

Note - any comments you may want to add about this entry. If you are creating a new note entry, this is where you write your important information you are about to store.

Advanced properties

In *Account/Note Properties* window there is also **Advanced** button, it expands the window and displays few additional (less used) fields:



Template - Specifies autofill template that is used by *Autofill* function. Don’t change this if you don’t know what you are doing. See “Automatically filling login prompts” topic for more information.

Expires - This field allows you to assign an expire date to the entry. Basically this may be useful for password accounts that expire after certain date but also for system admins who store their workgroup user accounts in a *Password Agent* database. To display popup calendar that allow you to easily pick up a date, click on the down arrow button. To remove *Expire Date*, uncheck the checkbox in the date picker control. If *Expire Date* is specified and **View | Highlight Expired Entries** option is activated, *Password Agent* will color code expired and soon to expire entries in main listing with colors specified under *Options* (red by default).

The button next to the *Expires* field displays popup menu that allows you to easily set a future expiration date. Default entries are *15 days*, *1 month*, *3 months* and *1*

year but **you can specify different time values by editing template** in “Password expiration” section under program options.

Old password - This field displays your old password, if present. That is the password that was associated with the account before you assigned current password. *Password Agent* just remembers one level of old passwords automatically, just in case something happens and you need to access your old passwords. This field is read-only and visible only if there is an old password available for the account entry you are viewing. If you are creating a new account entry you will not see this field.

Added – displays date the entry was added to the database. If no date is displayed, it is possible that this entry was created with an early version of *Password Agent* that did not record date of addition.

Saving your file

Saving your file is done automatically each time you change any information, so there is no separate *Save* command that can be triggered by the user. This reduces the risk that your computer crashes and you’ll lose important changes in your data.

Once saved, any previous version(s) of the file will be available with the extension .oldN, where N is number from 1 to 9. By default the program keeps 3 previous versions of the file -- .old1 being the newest and .old3 being oldest. Each time file is saved, oldest version is deleted. That of course does not mean that you should not make backup of your password database. Always make a daily backup of your data files off your computer since if your computer crashes you’ll lose all data. You can configure how many copies of old files to keep on Main tab of Options.

Tip: *Password Agent* can automatically copy your data file to an alternate location, like different folder or different computer in a local network. See “Main tab” (page 25) on how to activate and configure this feature under program Options.

Undo feature

Password Agent has one level undo feature that allows you to undo mistakenly invoked delete, edit or move actions. Right after you have mistakenly carried out one of the editing, moving or deleting commands, choose **File | Undo** command do undo the action. If you have deleted two or more entries in row, you can only undo last deletion, so be careful with potentially dangerous editing functions.

Opening a file

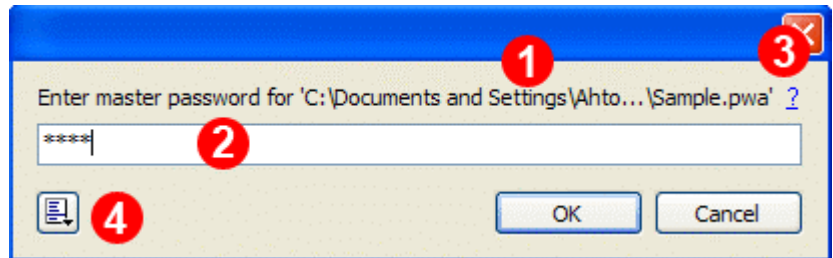
If you work with only one file, then you usually don't need to open the file manually, *Password Agent* automatically opens the file you used last time at startup. You can override this under *Options* by specifying your custom startup file (see “Main tab” on page25).

To open a file:

1. Choose **File | Open** command and select the file you want to open.

Now *Password Agent* asks for the master password of the file by displaying Unlock window presented below. You need to type in your

master password, so *Password Agent* can decrypt the file and display its contents.



1. Your data file name. By default you see file name with full path (it's folder name). If you want to see only filename without full path you can change *Show full data file path in Unlock window* setting in program options. If full path is not visible because it does not fit the label then hover the mouse pointer over the label and full file name is displayed as popup hint.
2. Master password input box, type your master password here. Master password is case sensitive, so be sure you have your keyboard's *Caps Lock* function inactive when typing it.
3. If you have assigned master password hint to your data file you can see the hint as tool tip when moving your mouse over "?" label at right or by clicking "?" with the mouse. This label is visible only if you have master password hint set.
2. After typing in your master password press the **OK** button to submit your master password. If your password is valid, the file is decrypted and displayed, if not you'll see an error message and can try to enter your password again.

Options button (number 4 on the above image) lets you override global *Master password input box type* option for just this login. See *Master password input box type* option (page 27) for more information about available options and their effect. By choosing input box type here you are not changing global setting but just override global setting for one time for this login. If other than *Custom with key logger prevention* is selected, Options button image contains warning overlay. This lets you easily notice when this setting has been changed to less secure choice (either by you or someone else). For example, someone can change your program option to disable key logger prevention to try to capture your master password using key logger.

Security features

Password Agent has several security features that help you to keep your sensitive data private.

- Your entire database, where the data is stored is encrypted with strong AES (Rijndael) algorithm using 256-bit key that is created using Haval algorithm. Rijndael was chosen lately as U.S. government encryption standard to replace older DES encryption format and is now called AES (Advanced Encryption Standard).
- Key logger confusion. Starting from version 2.6, *Unlock* and *Set Master Password* windows where you enter master password are doing some additional work behind the scenes to combat spy programs and key loggers. The password you type is not recorded by key loggers in

plain text as it was typed. Instead, *Password Agent* will generate random characters after each key press, so it is more difficult to detect real password that you entered. However, as it is not possible to hide keyboard input from key logging programs your real typed characters will still be captured by logger, so if logger can record several password entries over time, real master password can be discovered after some analysis.

Edit box for master password does not have ES_PASSWORD style, it does not allow copy & paste and does not give away your real typed password in response to WM_GETTEXT message.

- With each failed attempt to open data file with invalid password open procedure will be delayed by 3 seconds. So after trying to open the file with wrong password for 10th time you'll need to wait 30 seconds until you can try again. Even if you close the program between attempts the delay will not be reset. It will be reset if you restart Windows.
- If wrong password has been entered more than 2 times before file is finally opened with correct password, you'll see message box telling you that someone has tried to get access to your file. This feature only records attempts that are made on local computer since start of current Windows session.
- Sensitive data kept in memory is scrambled.
- The program is automatically locked when screensaver activates (option). In addition you can specify the program to lock or close itself after period of inactivity (see "Lock/close timer").
- By default, all sensitive information is hidden - *UserID*, *Password*, and *Note* columns display a "#" symbol instead of the actual data in entries listing. This protects your privacy if someone watches your screen from behind you, or over your shoulder. They will not see your private data, as only the "#" symbols are visible. If you want to display the actual information instead of the "#" symbols, choose **View | Mask Sensitive Data Columns** command. This option toggles the data displayed on and off. You can also specify which columns exactly will display "#" symbol instead of the actual data by right-clicking the column's header and choose **Sensitive Information** from the popup menu.
- There is also a function that deletes all text that you may have copied to the clipboard and the clipboard text is deleted automatically when you exit the program, or the specified timeout occurs. See the "Security" topic on page 26 for more information.
- Supports CF_CLIPBOARD_VIEWER_IGNORE clipboard data type. If you use compatible clipboard manager (like [ClipMate](#)), this instructs the clipboard manager not to capture passwords and sensitive data copied to the clipboard from Password Agent.

Warning: There are no backdoors in the program, so if you forget your master password, even we can't help you to open your file. So be careful with your master password.

Locking a file

The **File | Lock** function allows you to lock your open file and *Password Agent* without closing the program. If a file is locked, *Password Agent* is minimized and its icon has a little red lock overlay. Any attempt to restore the program will cause the program to prompt for the master password. The prompt is very similar to the one that you see when opening a file (see “*Opening a file*” on page 17) except it has additional button titled *Release Lock*. The *Release Lock* function allows you to remove the lock from the program, without opening the locked file.

The program has also several options that allow you to specify whether the program will lock or close itself automatically, after specified period or user inactivity or when screensaver starts. See Main tab under *Options*.

If the program is locked, current file is unloaded from memory for advanced security.

Warning: If the program is automatically locked by user inactivity, any pending editing is discarded. That means if you are inserting a new entry or editing an existing one, then leave your computer for a long time and the automatic lock/close option is enabled, your changes will be lost. Always finish adding or editing an entry then you leave the program.

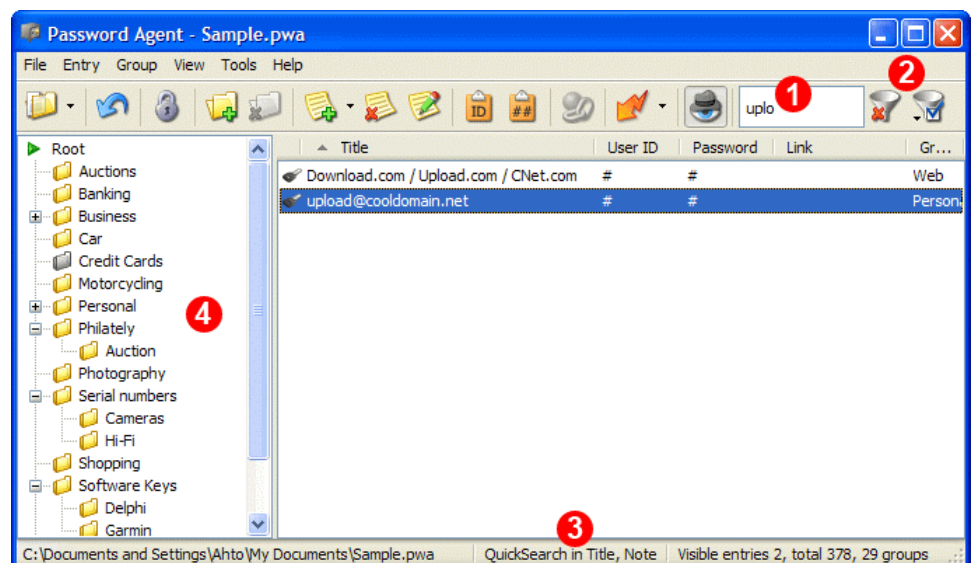
Searching

Password Agent makes it easy for you to find your entries – you can use either the *QuickSearch* filter or the *Find* tool.

When QuickSearch is active, clicking any group in groups tree will cancel search and display contents of clicked group instead of search results.

Using QuickSearch

QuickSearch is very easy to use and gives excellent results quickly. Basically you enter a phrase or part of the name of an entry you want to find and *Password Agent* filters its entries as you type to match your query.



1. You type the text you want to find into *QuickSearch* box, entries list will reflect and will display only entries that match your query. In that example you see that only entries that contain phrase “uplo” are displayed. To jump into entries listing you can press **Enter**.
2. To cancel your search, press this button or press the Esc key when focus is in *QuickSearch* box or Alt+Q when focus is elsewhere.

Second button after *QuickSearch* box displays *QuickSearch* options. You can choose what fields should be searched by *QuickSearch* function. By default only *Title* field is searched for match but you can add any other fields you want to search. This setting is saved between sessions, so next time *Password Agent* uses the same options you have selected in the popup menu.

3. Status bar displays message while *QuickSearch* is active. On this picture you see on status bar that *QuickSearch* searched for your phrase in *Title* and *Note* fields. To define what fields should be included in the search use *QuickSearch options* menu (under last button).
4. When *QuickSearch* is active, clicking any group in groups tree will cancel search and display contents of the clicked group instead of search results.

When you open a file, input focus is automatically moved to *QuickSearch* box, so you can start typing there immediately.

Tip: Use unique search phrases – for example if your entry is titled “ShareIt”, you don’t need to start typing “share” into quicksearch box, as it will also return other titles that contain the word “share”, like “shareware” etc. To find your entry quickly and with less typing use unique phrase the entry title contains -- instead of typing “shareit”, you can just type “reit”, or for example if your entry title is “Microsoft Passport”, you can type “ssp”, as not many other titles contain phrase “ssp”. Also, you can make your own unique keywords and add them to the end of entry title. For example you can add keyword “msp” to your “Microsoft Passport” entry, so it will be displayed as “Microsoft Passport (msp)” and you’ll find it quickly by typing “msp”.

Tip: You can use **Ctrl+Q** shortcut key to activate the *QuickSearch* text box and **Alt+Q** to cancel QuickSeach. If input focus is in QuickSearch box, **Esc** will also cancel search mode.

Using the Find tool

The Find command allows you to search for entries that match your criteria.

1. Choose **Entry | Find** command, search window is displayed.
2. Enter the text you want to search for (search string) into the *Text to Find* box.
3. Press the **Find** button.

If an entry matches your search criterion, it will be highlighted. To quickly find the next match, you can use **Entry | Find Next** command or press **F3**. That will re-use the same search settings, and will try to find the next entry that matches your search criteria, after the currently selected entry.

You can perform advanced searches by specifying wildcards "?" in your search string. "?" means that there may be any character at that place. For example, if you want to search for both "biking" and "boxing", you can use search string like "b??ing".

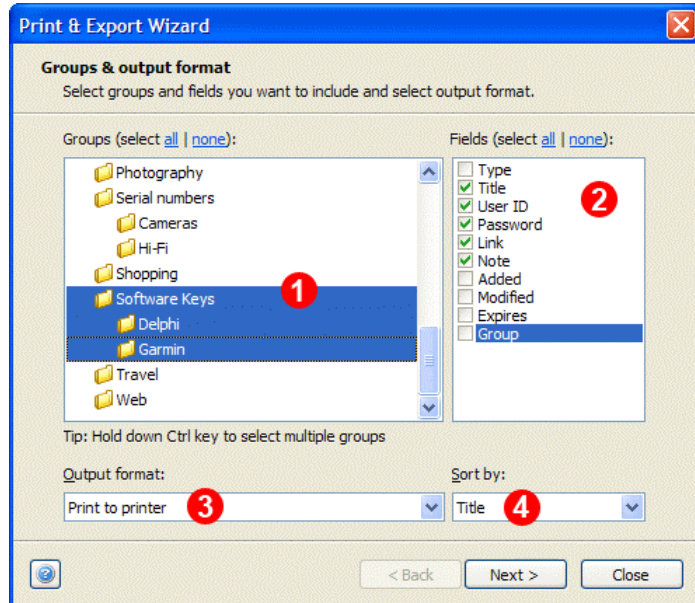
Note: Search starts from the selected entry and goes to downward. If no entry is selected, searching starts from the topmost entry.

Note: The *Password Agent* search function is not case sensitive.

Printing

Password Agent allows you to print your password entries using the *Print & Export Wizard*. You can specify what groups and fields to print, select sort order, font etc.

1. Choose **Print & Export Wizard** command from the **File** menu. You'll see the following window:



- 1.1 Select groups you want to include in your printout. Hold down the Ctrl key when clicking with the mouse to select multiple groups. Also, you can click-drag with the mouse to select multiple continuous items.
 - 1.2 Select fields you want to include in your printout. Click check boxes with the mouse to toggle check state.
 - 1.3 Leave "Print to printer" as output format. You can select different output format to export data in different formats. See "Export" on page 36 for more information about exporting.
 - 1.4 You can order items by different fields like in the main entry listing, but most likely you want to sort by *Title* when printing.
2. If you have selected desired groups and fields then press **Next** button to continue.

3. Change printer and font settings if required, and then press **Print** button to start printing with the selected settings.

Here is a sample fragment of a printout. All data is placed between double quotes to make it easy to distinguish between fields:

```
01. "Amazon.com" "test123" "dDgGfKpp" "http://www.amazon.com/" "Amaz
02. "Barnes & Noble" "test" "yUOIq4s5" "http://www.bn.com/" "Buy boo
03. "EzyDVD" "testuser" "QqXTRG0R" "http://www.ezydvd.com.au/" "Chea
```

Tip: If you want to print more complicated reports (tabbed columnar or grouped) you can export data into HTML format and print using your web browser. See “Export” on page 36 for more information about exporting data into different formats.

Sorting

You can order (sort) entries in the list by different criteria: by title, by account, by date etc. By default, entries are sorted by Title. It is very easy to change the sorting order:

1. Click the column header you want the data sorted by. For example, click the *Date* column to sort by date added. You will see the latest entry listed first. To sort by *Title*, again click the *Title* column header. It is that easy!

You can also sort in descending order. If your data is sorted by *Title* for example, clicking the *Title* column header again will sort by the same column, but in opposite order (i.e. by *Title*, but now in descending order).

Another way to change sort order is through menu: **View | Sort By**.

Hiding and reordering columns

Password Agent allows you to easily reorder and hide columns that you see in the entries list. That way you can display only the information that you are interested in, at the place where you want the info displayed. For example, you can hide *Date* and *Link* columns if you don't usually use those fields. Hiding a column does not delete any data - you can still access all fields if you want to edit an entry.

To display column customization window:

1. Choose **View | Columns** command or right-click on column heading and choose the Columns command from the popup menu

The *Columns* window consists of 2 list boxes: *Available* and *Visible*. In the *Visible* list box you can display only the columns that you want to be visible. You can move an item to the other list box, by double-clicking on it with the mouse, or use the special buttons located between the list boxes.

The *Visible* list box allows you to reorder items by dragging them with the mouse. That way you can order the visible columns the way you want. The topmost item is displayed first.

The Defaults button will restore default columns.

2. After you are done with customization, press **OK** button to see the results. If something looks wrong, you can display the *Columns* window again to make any corrections.

Tip: To quickly reorder a column without opening the *Columns* window you can drag column header with the mouse to a new position, then release the mouse button.

Useful tools & functions

Password Agent has few simple but useful tools.

Tools | Password Generator – Invokes password generator.

Tools | Clear Clipboard - Clear the clipboard.

Tools | Export Registry Settings – This command allows you to export *Password Agent* registry key to a disk file that can be merged with the registry in another computer (.reg file). That way you can easily transfer all current program options and settings, excluding key code, to another computer(s).

File | Backup/Copy to - Simple function to help you to copy the currently opened file to another location. We suggest that you save your files in a central work folder, like "My Documents" and then use backup software (like our own [Backup Magic](#) program) to make regular backup of all your work files. If this is not your normal practice, you can use this very simple method to make a copy.

File | Place Shortcut on Desktop - Creates a shortcut to the current file on the Desktop.

Entry | Duplicate – This command allows you to make an exact copy of the selected entry. Useful if you want to create a new entry similar to an existing one.

Entry | Convert Type – This function allows you to convert from one entry type to another, from note to account or vice versa.

Help | Check for Update - allows you to check for program updates. Choosing this command will open your web browser and tries to connect to the Moon Software web site to check if there is a new version of *Password Agent* available.

Password Generator

Password Agent includes a special tool that allows you to easily generate new, difficult to guess random passwords. You can use it to generate passwords for new entries or just as a stand-alone tool to generate passwords used outside *Password Agent*.

To invoke stand-alone *Password Generator*, use **Tools | Password Generator** command. If you need to generate new password for a new or existing entry, there is *Generate password* button in "Entry Properties window" right after the *Password* field.

The *Password Generator* has two different password generation methods. To change password generation method, just select right tab.

Quick method just needs to know how long password do you need and what kind of symbols to include.

Template method is more powerful, there you can specify exactly how many symbols of each kind do you want to include and their positions. Optionally you can

shuffle passwords, making them more random (more secure). When password that is generated by template is shuffled, it will use the same number of certain symbols as specified in the template, but in random order.

The **Save all settings as defaults** checkbox (visible when you extend the window by pressing *Options*) allows you to save your current settings as default settings for new passwords. If this checkbox is selected, the next time *Password Generator* will use the same settings and also all your automatically created passwords for new entries will be generated using these settings. Password generation method (either quick or template) will be also saved accordingly which tab is selected.

Tip: Don't use short passwords, they are not secure. The longer and more difficult to remember a password is, the more secure it is. With *Password Agent* you can use long and complicated automatically generated passwords because they will be remembered by the program, not by you. You only need to fight with your master password.

Options

There are several options you can set to further customize the program to your needs. Display the *Options* window by choosing **Tools | Options** command.

Tip: You can restore factory settings any time by pressing the *Defaults* button in the *Options* window. *Password Agent* will then prompt to restore all settings or only settings on current page.

Main tab

Tip: To load default value for any single option item or even entire group, right-click on the item or group and choose **Restore default value** from popup menu.

View

Always expand Properties window automatically – Automatically expands the *Properties* window, so you don't need to manually press the *Advanced* button. By default, advanced fields are only shown when they contain data.

Use system font (requires application restart) – By default *Password Agent* uses system font in all its windows. It is the same font that *Windows Explorer* uses (by default *Tahoma* in new systems). If you uncheck this option then *MS Sans Serif* font is used.

Expand all groups on startup - If set, the groups tree is fully expanded after opening file. Otherwise, you only see the first level of groups. If you wish, the Groups menu in the main window has commands to expand and collapse the groups manually.

Show entries from all groups in the root group – By default, if you activate the Root group, entries list displays all entries from all groups. By unchecking this option you can make the Root group display only entries that reside in the Root group (actually entries that are ungrouped, i.e. they have no group assigned).

Functionality

Minimize to system tray - Specifies whether icon are displayed in the task bar tray area (near the clock). Also, if this option is set, minimizing the program will hide it from the task bar, you will only see its icon in tray area.

Minimize after autofill – Specifies whether the program automatically minimizes after automatically filling a login prompt.

Save window size & position on exit – If this is checked then the program will save its position on exit and will start next time on the same screen position. You can use this option to save “ideal” program window position, then uncheck it so further position changes will not be saved. *Please note that window position is not saved when the program window is maximized. That is intentional, taking into account the fact that you probably don’t want to use the program in full screen when you start the program next time.*

Generate passwords for new entries automatically – Specifies that *Password Agent* will automatically generate password when you create a new account entry.

Close to system tray – If specified, the program will minimize itself to system tray when X button of the main window is clicked, instead of closing the program.

Copy password to the clipboard on Open Link – When active, password will be copied to the clipboard when you use the **Open Link** command. Then you can paste the password to right place on the web page. Useful if autofill is not working with the site or you just prefer to enter password and user ID manually.

Show full data file path in Unlock window – This option controls if you see full path including drive and folder of your data file name in Unlock window where you enter master password or file name only.

Security

Lock program when minimized - Specifies that the program will be automatically locked if you minimize it (the same as **File | Lock** command). If you also have *Minimize after autofill* option set, then the program will be locked after autofill.

Lock program when screensaver activates – This option causes the program to lock your file when screensaver activates. This prevents other people to see your sensitive data if you are away from your computer. *This option is not available on Windows 95 and NT. Use “Lock timer” on these platforms to automatically lock the program.*

Mask sensitive data columns on startup – Automatically invokes **View | Mask Sensitive Data Columns** command every time the program is launched.

Clear clipboard 2 minutes after copying data - Specifies that the program will automatically clear text we copied to the clipboard 2 minutes after copying. That affects only text we have copied from *Password Agent*, not text copied from another programs.

Clear clipboard on exit - Specifies that text from the clipboard is automatically erased when the program is closed. That affects only text we have copied from *Password Agent*, not text copied from another programs.

Clear page file at shutdown – This option will force Windows to clear page file when computer is shutting down, improving security. This may delay Windows shutdown process. Please note that if computer is simply switched off or crashed, then this process is not carried out. More information about security is available in “How secure?” topic on page 6. *This option is available only on Windows NT/2000/XP/Vista/7 and requires administrator privileges.*

Lock/close timer

Here you can specify timeout (in minutes) of inactivity, after what the program will either lock or close itself. You can't select both lock and close options at the same time, but can select none of them. If none is selected then the lock/close timer will be disabled.

Master password input box type

Starting with version 2.6 *Password Agent* contains function to protect your master password from logging by key loggers and spy programs. For this *Password Agent* generates additional hidden keystrokes that are mixed with your typed master password, so key logger records random characters in addition to your real master password. Unfortunately, on some systems (where keyboard rate is set to very high and password is typed very fast) this approach may interfere with your real master password causing it to be rejected, so you have option to turn this function off.

These options only affect *Unlock* window where you enter your master password and *Set Master Password* window where you can change your master password.

Custom with key logger prevention – Custom password input box implementation that prevents text to be captured by other programs. Copy and paste from input box is also disabled. Key logger prevention is active. This is default option.

Custom without key logger prevention – Same custom input box implementation as in previous option but key logger prevention is disabled. Select this option if default key logger prevention causes problems like frequent *invalid master password* prompts.

Classic (not secure but compatible with 3rd party software) – This option uses Windows classic password input boxes that were used in *Password Agent* 2.5 and earlier versions. These are less secure than custom implementation as other software programs can easily capture text entered and key logging programs can easily detect that you enter password, not usual text. Use only if you need compatibility with other software or custom implementation causes problems.

Startup

Settings here tell *Password Agent* what file needs to be opened when you start the program.

Load automatically on Windows startup - Check this if you want *Password Agent* to start with *Windows*. *Password Agent* uses smart startup; on startup it is minimized and does not prompt for master password until you want to actually use it. Putting a shortcut in the *Windows Start Up* group does not solve this problem, unless you specify **/minimize** switch on the *Password Agent* program command line (see “Command Line” for more information).

Action on double-click

Here you can define what happens when you double-click on an entry in the entry listing. Possible choices are: **Autofill** (equals Entry | Autofill), **Properties** (default, equals Entry | Properties), **Copy Password** (equals Entry | Copy Password) or **Open Link** (equals Entry | Open Link).

Pressing Esc key will

Here you can define what happens when you press **Esc** key in main window. Possible choices are: **Lock program** (equals File | Lock), Minimize program

(default), **Exit program** and **Hide Sensitive Information** (equals View | Mask Sensitive Data Columns).

Backup

Count of old files (.old1, .old2 etc) to keep when saving – The program can keep specified number of old versions of the file when saving. Useful for backup purposes but can slow down the program a bit. See “Saving your file” for more information.

After saving file copy it to the following folder – By checking this checkbox and by providing a valid file name with full path in the following text box you instruct *Password Agent* to copy your file to alternate location after saving file. For example, you may specify a network path here, so each time you save your password database it will be automatically copied to another computer. That way you always have up to date backup if something happens with your main file.

Please note there are some issues with this. Since the program will automatically save your file after every (even the smallest) change, if you are copying to a slow device this will slow down the program. Also, if something happens to the file during saving so it becomes damaged, it may happen that the damaged file is copied. So this command does not fully replace manual (and frequent) backup of your data file.

Password expiration

Warning days – *Password Agent* can highlight entries that will expire after day count specified here. Highlighting occurs only if you have **View | Highlight Expired Entries** setting active. See “Using expiration date” on page 35 for more information.

Expire date popup menu template – By modifying this template you can configure what entries will be included in popup menu that is displayed by clicking button next to *Expires* field in “Entry Properties window” (see page 15) . The popup menu allows you to quickly set password expire date using pre-defined periods, like after 30 days, 3 months, 1 year etc. The default template is 15D 1M 3M 1Y and this will produce the following entries in the popup menu: 15 days, 1 month, 3 months, 1 year. If you are not satisfied with the pre-defined menu entries, you can change the template here to include different time values. Rules are that you need to write number, followed by D (days), W (weeks), M (months) or Y (years). Multiple entries need to be separated by a space. To change the popup menu to include only 10 days and 2 weeks entries, use 10D 2W as template here.

Message boxes

In this section you can enable/disable some of the warning messages *Password Agent* displays. Disable them only if you are sure what you are doing.

Colors tab

Expired password color – Specifies color that is used to paint expired entries when View | Highlight Expired Entries setting is active. See “Using expiration date” on page 35 for more information.

Password expire warning color – Specifies color that is used to paint entries that will expire soon. Color coding is only used when View | Highlight Expired Entries setting is active. See “Using expiration date” on page 35 for more information.

Even rows color - This allows you to make all even rows colored, so you can separate entries more easily. If you don't want to color even rows with separate color, choose “*Window*” color here.

Templates tab

Templates tab allows you to change default autofill templates. Default templates are used when you have not assigned a custom template to an entry. See “Automatically filling login prompts” on page 30.

Hot keys tab

Here you can assign system wide hot keys to activate *Password Agent* or its function when it is not currently active application on your screen. *Password Agent* must be running on background (may be minimized, or in tray) for these to work.

Activate Password Agent – This hot key simply will bring up *Password Agent* if it is minimized or not topmost application on your screen.

Autofill – Will use *Autofill* feature to send text to active application. Invoking *Autofill* using a system wide hot key is a very handy feature, see “Autofill using global shortcut key” on page 31.

Autofill password only – similar to previous but will only send password.

Common User IDs tab

Here you can specify your most commonly used user IDs. These will appear in the *User ID* drop-down box in *New Account* window for easy access, so you don't need to re-type your user ID manually when creating a new account entry.

Use the first ID from the list as default for new entries – Allows you automatically fill *User ID* field when creating a new account entry.

Multiple users

Multiple users can use *Password Agent* without problems. Since *Password Agent* can operate with different disk files, every user can create personal password database file. Then everyone can place shortcut to his or her file on the Desktop for example (open desired file, then use the **File | Place Shortcut on Desktop** command). Next time you want to access your file, you can just double-click your shortcut.

Note: *Password Agent* database files are not designed for use in network environment by multiple people at the same time. Only one process can open a file for saving, so if one user has opened the file for editing, another user(s) over network can only open the file in read-only mode and can't make changes.

Tips & tricks

Quick Launch vs. System Tray. Many people keep a lot of programs running in the system tray area (on taskbar near the clock). *Password Agent* can also be locked into system tray. The programs are easily accessible from system tray, but they also take your computer resources (processor, memory, startup time etc) because they are actually running on the background, so it is recommended to have only the programs that really need to be there. Starting from *Windows 98* there is another area on the taskbar called *Quick Launch* toolbar. You can put shortcut to your *Password Agent* data file into this area, so you can access it as fast as from system tray (when the program is locked). And instead of auto-lock timer use auto-close timer. Then the

program will be closed after inactivity, not locked. Since it takes same effort to open locked *Password Agent* or opening *Password Agent* file from shortcut when it is not running, it makes sense. But if you keep *Password Agent* in system tray in unlocked form for quick (keyboard shortcut) access, then you can't take advantage of this suggestion.

Errors in the program. If you see *Access Violation*, un-handled error message or the program just misbehaves, it is strongly recommended that you close *Password Agent* and restart it – do not continue to use it even it seems to work okay. That way you can prevent your data file from potential corruption. If the problem is continuous, please report it to our tech support.

Advanced Features

Automatically filling login prompts

Note: This feature is for advanced users.

One exciting *Password Agent* feature is the ability to fill in login prompts (web sites, software programs) automatically with your user name and password or other data you have stored in the database. But this feature has also limitations, so be sure to read and understand this entire topic if you plan to use this feature. **While some programs can completely automate logins by integrating themselves into web browser, *Password Agent* requires you to select where you want to enter text and from which database record. So it is much less automated than some other similar programs, but on the other hand it is not integrated with any web browser so you can use it with many different browsers and move from one computer to another without need to configure something.**

Password Agent uses "send keys" method. That means it will try to simulate keystrokes, as you were entered the text yourself. Most login prompts consist of 2 text boxes: user name and password. Typical scenario is that you fill both boxes, and then press a button to log in. *Password Agent* can save you of typing your user name and password manually - you can instruct it to fill in such login prompts (forms) for you. But there are a few problems with this:

- Login form may have different layout than simple user name and password text box. For such forms, you can manually edit template so you can send data to complicated forms without major problems. Template allows you to teach *Password Agent* how to act with non-standard forms. By default, *Password Agent* uses default template for all entries, but you can manually edit it for entries that must act different.

- When using basic autofill (scenario 1 below), *Password Agent* needs to know into what application you need to enter data. This can be only solved if you activate this application, then switch into *Password Agent*. *Password Agent* then knows the application you want to send data to is the one that was active before you activated *Password Agent*.

Autofill using global shortcut key

This is preferred method since it is more flexible.

1. Open *Password Agent* or switch to *Password Agent* if it is already open.
2. In *Password Agent*, find entry that contains information you want to transfer and select it.
3. Open desired web page in a web browser or run the program that requires you to enter password. You can minimize *Password Agent* but don't close or lock it. You may use *Password Agent*'s *Open Link* function. In fact, this is the best place to make use of the *Open Link* function.

Activate the user name/account text field so you see cursor blinking there. This is important because then *Password Agent* knows from what field to start entering data.

4. Press the system wide (global) autofill shortcut key combination, defined in **Tools | Options** window, Hot keys tab (see page 29). Default key combination is **Ctrl+Shift+A**. That means you need to hold down both Ctrl and Shift keys and press the A key at the same time. If all is OK, you see fields will be automatically filled for you.

If nothing happens or another program pops up when you press the global autofill shortcut then most likely another program is using the same key combination. Go to Tools | Options and try using a different key combination.

See also "Sample workflow using autofill" on page 32.

Basic autofill

1. Open desired web page in a web browser or run the program that requires you to enter password
2. Activate the user name/account text field so you see cursor blinking there. This is important because then *Password Agent* knows from what field to start entering data.
3. Open *Password Agent* or switch to *Password Agent* if it is already open. Note that if you activate any other applications now, data transfer will fail because your program that contains your login form must be active program before you switch to *Password Agent*.
4. In *Password Agent*, find entry about your web site, select it, and choose the Entry | Autofill Login Prompt command. If all is OK, you see your web browser/program is activated and both user name and password fields will be automatically filled for you.

Sample workflow using autofill

Here is sample workflow that allows you to fill a login prompt on web site **using keyboard only**. We also use QuickSearch feature. We assume you have *Password Agent* running on screen and you have your password database file already open.

1. Press **Alt+Q** to activate the *QuickSearch* box.
2. Type in part of your entry name so the desired entry will be displayed in entry listing.
3. Press **Enter** to jump to entry listing. If you have only one entry displayed in the listing then it is probably the right one. You can use **Up Arrow** or **Down Arrow** keys to select a different entry.
4. Press **Ctrl+K** to invoke *Open Link* command. That will open web site associated with the entry. If you have not filled in the entry's Link property then you'll need to open your web page manually.
5. Activate the user name/account text field on your web page so you see cursor blinking there. This is important because then *Password Agent* knows from what field to start entering data.
6. Press the system wide (global) au tofill shortcut key combination **Ctrl+Shift+A**. That means you need to hold down both Ctrl and Shift keys and press the A key at the same time. If all is OK, you see fields will be automatically filled for you.

Tip: You can change the system wide shortcut key under Options, Hot keys tab (see page 29).

Templates

Template is a series of instructions, how *Password Agent* should send text to another applications. As mentioned earlier, *Password Agent* activates another application and simulates keyboard events to enter text into that application. By default, the following sequence is used:

```
User ID <TAB key> Password
```

That means typing your user ID, then simulating Tab key pressing (to jump to the next text box) and finally typing your password. If you open *Properties* of an entry then pressing the *Advanced* button will display few more fields of an entry, including *Template* field. The default template for account entries looks like this:

```
$USERID{TAB}$PASSWORD
```

`$USERID` variable will be replaced with your actual data from *User ID* field, `$PASSWORD` variable will be replaced by your actual password and `{TAB}` variable is special instruction to simulate Tab key on the keyboard. In addition you can use the `$NOTE` variable to send text from *Note* field, but that is probably used only little. If your form requires you to press Tab several times to activate right text box, you need to include the same amount of `{TAB}` variables or use special instruction `{TAB n}` where *n* is number of Tabs to enter.

For example, this slight modification automatically presses **Enter** key after filling in your form, so the form will be submitted after filling. Also, it presses Tab 2 times between *User ID* and *Password*:

```
$USERID{TAB 2}$PASSWORD{ENTER}
```

To insert pause between sending some data, you can use special {WAIT} variable. Each {WAIT} variable will make 0.5 sec pause. You can also specify length of pause by specifying milliseconds. The following variable will pause for 1 second: {WAIT 1000}. Generally, you don't need to use the {WAIT} variable, it is provided for special cases. The following example will wait 1 second after sending user ID and pressing enter, then will send password and another enter:

```
$USERID{ENTER}{WAIT 1000}$PASSWORD{ENTER}
```

You can basically mix variables and plain text in template. If you need to send several strings, you can also hardcode them into the template, like:

```
$USERID{TAB}Text1{TAB}Text2{TAB}$PASSWORD{ENTER}
```

That may be useful for some advanced login prompts that may require you to provide more info than just user ID and password.

Note: If you have modified the template, the template field is visible automatically if you display the *Properties* window. If you have not modified the template, the template field is not visible by default, but you need to press *Advanced* button in the *Properties* window to see it.

Note: If you use *Internet Explorer* 4 or newer and want to use *Autofill Login Prompt* function, you should disable *AutoComplete* feature for passwords and user names in *Internet Explorer*. If you don't disable *AutoComplete*, both *Internet Explorer* and *Password Agent* try to fill a form at the same time, so you end up with wrong text entered. See readme.txt file for more info how to do this.

Tip: You can modify the default template in *Options* window, *Templates* tab. For example if you want *Password Agent* to always automatically press Enter after filling out the form, you may change the default template to:

```
$USERID{TAB}$PASSWORD{ENTER}
```

Taking the program with you

TakeWithMe wizard

It is possible to take *Password Agent* and your password database file(s) along with you, you just need to copy them to a removable disk (floppy*, USB flash disk etc) that you carry with you. That way your passwords and secrets are always with you and you can run the program off the removable disk - you don't have to install it on target computer. Only main executable file is required to run the program, although you can also include help file or any other files.

TakeWithMe wizard makes it easy to prepare or update your removable disk. To run the wizard you'll need to have your data file open, then select **File | TakeWithMe**.

Which files to copy – here you can select which files you want to copy. The **Key code** item allows you to include your key code in INI file, so your program will be always started as *Unlimited* version, not *Lite* version, even on computers where there is no *Password Agent* installed. The **Key code** item is disabled in *Lite* version, because *Lite* version has no key code.

Also, when copying your data file, previous versions will be available as .old files, similar to saving files. So if you accidentally overwrite important data on removable disk, you can still access the .old files.

Target drive, folder or disk label – here you need to provide your target drive, where selected files will be copied. One nice feature here is that you can also specify disk label**, not drive letter. That is useful for devices where drive letter may change depending how many other removable disks you have connected at the moment. Specifying your USB flash disk label here will insure that files will be copied to it regardless its current drive letter.

Save settings – check this box to save current settings as defaults for next time you run the wizard. Then next time you'll only press Start and everything is copied automatically.

* Classical floppy disks are not recommended because they are very fragile and you may soon discover your important data file is damaged. USB flash disks are ideal choice, because they are high capacity, fast, compact and reliable.

** Disk label search will start from letter C. It can't be used with A and B drives. These drive letters usually don't change anyway, so you can just use "A:\\" or "B:\\" as target folder. If there are multiple disks with the same label, first of them will be taken.

Running Password Agent from removable disk

Password Agent has some special features when the program is started from a removable disk:

- If there is a data file in the application folder, *Password Agent* will open it by default.
- If there are more than one data file in the application folder, the program will prompt which one to open.
- On startup, default options will be used if the program detects alien computer.*
- Program options will not be saved to the registry if the program detects alien computer.**
- When using unlimited version of *Password Agent*, you can copy your key code to the application folder, then the program will always start up in unlimited mode, even you are using it on alien computer where unlimited version is not present.

* Other people may have configured the program the way it is very unfamiliar to you. In addition, some of your sensitive information may be visible if other people have not specified sensitive columns at all, etc. Also, because *Password Agent* allows you to make automatic backup copy of a data file when saved, that will prevent your data file to be copied to other user's backup location, etc.

** That is to protect other people so you will not overwrite their *Password Agent* options. That will also help to keep the registry clean of unwanted settings on alien computers where *Password Agent* is not installed at all.

How Password Agent detects alien computer?

Every computer where there is no key code in the registry or where key code in the registry will not match the key code stored in the application folder on removable disk is considered alien computer.

That also means the free *lite* version of *Password Agent* is unable to save settings when started from removable disk, because it does not have key code used to compare computers.

Using expiration date

Password Agent allows you to set expiration date of an entry. This is useful for system administrators who keep accounts of multiple users in their *Password Agent* database, so they can get visual notification when accounts are going to expire.

You can set/remove expire date by changing *Expire date* field in the *Properties* window:

1. Choose **Entry | Properties** to start editing an entry.
2. Press the **Advanced** button in the *Properties* window if *Expire date* field is not visible.
3. Choose desired expire date using drop-down calendar control. To remove previously set expire date uncheck the checkbox in calendar field. To increase the date using certain amount of days, like 30 days, right-click the *Expires* field and choose specific command from popup menu. Also note that you can change time periods displayed in the menu under *Password expiration* section in program options.
4. Press **OK** to apply changes to the entry.

Password Agent can color code entries that are expired and that will expire soon. That way you can easily see which entries are expired or will expire soon.

1. The **View | Highlight Expired Entries** toggle can be used to turn this color-coding on and off.

You can change highlighting colors on “Colors tab” under *Options* window.

You can change expire warning days in *Options* window, see *Password expire warning* section on “Main tab”.

Note: *Password Agent* only gives visual feedback about expired entries by highlighting them in different colors, it will not display any message boxes when an entry is expired.

Command Line

Password Agent command line syntax is the following (instructions between brackets are optional):

```
pwagent.exe ["file name"] [/minimize]
```

File name must include full path, put it between double quotes. If no file name is specified, the file that will be opened is specified by user under program options.

The optional **/minimize** switch can be used to force the program to start up minimized. Then it will not prompt for master password until it is restored. That is useful if you want to run it on startup.

Import & export

Note: If you need to move data from one computer to another don't use import and export! Just take your data file and copy/move it over (you can use **File | Copy To** command to copy currently opened data file). Import and export is provided to move data between different programs and may cause data loss.

Import

Note: This function is for advanced users.

You can import another *Password Agent* file or plain text file in CSV format. The latter allows you to import data from another password manager programs.

1. To import another file into your existing file choose **File | Import** command. To use this command you need to have an existing file open, then imported items will be added to the open file.

Warning: Import using CSV format is not bulletproof, so you should always check entries manually to make sure they contain the desired data.

Export

Note: This function is for advanced users.

Warning: Exporting entries from *Password Agent* results in an **unencrypted** plain text file (like CSV, HTML or XML) that is readable by most text editors. All your passwords are easily readable by anyone who opens the file with a text editor. So take care that those files are permanently deleted (also from *Recycle Bin*) after any export/import process.

The **File | Print & Export** function will launch *Print & Export Wizard* that allows you to print or export entries in popular CSV, HTML or XML formats. Printing and usage of *Print & Export Wizard* are discussed in the “*Printing*” topic (page 22) so we only talk about exporting in this topic.

Available output formats:

Print to printer – Outputs simple report on selected printer. Printing is discussed in the “*Printing*” topic on page 22. Printing a report through this command is secure since no unencrypted output is generated on disk.

HTML reports – It is possible to generate simple columnar or more advanced grouped HTML reports. HTML reports can be used to print advanced reports via your web browser since *Password Agent*'s default printer output is quite basic.

XML output –XML is the best export format if you want to transfer your data into a different database (program) since groups hierarchy is also saved.

CSV output – Export data in a basic “comma separated values” text file. No groups hierarchy is saved, but wide array of programs can import data in CSV format.

Keyboard shortcuts

There are some useful keyboard functions that are not associated with menu commands:

Spacebar – will scroll selected entry into view.

Backspace – will go to parent group. Alternative shortcut is **Alt+Left** or **Back** button on *IntelliMouse*.

* **on numpad** – toggle **View | Mask Sensitive Data Columns**.

Tip: You can configure the **Esc** key to your liking, see **Pressing Esc key will** under Options (“Main tab” on page 25).

Network installation

When sharing *Password Agent* on a file server you can use TakeWithMe wizard to generate INI file with key code and put this INI file on file server. That way everyone who will start *Password Agent* from the server will automatically have *Unlimited* version, you don’t need to manually enter key code in each workstation.

To make INI file, start *TakeWithMe wizard*, select only *Key code* checkbox and select target folder.

Note: When sharing *Password Agent* on server, you’ll need license for each user who runs the program off the server or site license.

Solving problems

Autofill feature does not work

The autofill feature is popular and powerful, but it may not work with all applications. Autofill is basically sending simulated keyboard input to another program, but depending on design of the target application, that may not work always. Some programs can't process keyboard input so quickly, others are not designed for this kind of input etc. While the autofill feature works with majority of applications, there may be some that do not seem to work.

Windows Vista/7 – autofill to certain applications completely fails. *Windows Vista/7* contains new security functionality that is called *User Interface Privilege Isolation* (UIPI). Among other things this means that you can't send user input into another application that runs with higher privileges than your application. Or in other words, if you run *Password Agent* as limited user (or under UAC), then you can't autofill to another application that has been started with administrator privileges. Windows Vista/7 does not allow this kind of communication and silently “eats” this autofill, so it will never reach destination application.

Also, on all Windows releases it is possible that **autofill does not work with certain application**, but works with others -- then usually problem is not in *Password Agent*. The target program probably uses non-standard input boxes that do not accept simulated input very well. If only part of the data (user ID or password only) is transferred to the target application, then you can try adding {WAIT} variable to your autofill template, something like \$USERID{TAB}{WAIT 500}\$PASSWORD{WAIT 500}. That will just give the target application a bit more time to process pending input. If that does not work, then you are out of luck and this application can't be used as autofill target.

If autofill does not work with any application then there are several options. First you'll need to find out if it is indeed problem with autofill, not problem of conflicting global hot keys. That means if you are trying to invoke autofill function by using global hot key combination (defaults to Ctrl+Shift+A), then please try again and this time use *Autofill* toolbar button. If autofill invoked by toolbar button works, then you definitely have problem with conflicting global hot keys and this is discussed in “*Autofill enters double/invalid password*” topic on page 39. But if the toolbar button did not seem to work either, you have got situation that is difficult to believe. If you have full understanding how autofill works and it does not, please contact support.

Tip: To figure out whether *Password Agent* misbehaves or is it your target application, try using *Notepad* as the target application. If everything is sent to *Notepad* properly, *Password Agent* works OK but you'll need to figure out why the target application does not accept input sent from *Password Agent*.

Autofill enters double/invalid password

If you want to use autofill function then you must disable your web browser's internal *AutoComplete* setting for passwords, otherwise both your web browser and *Password Agent* will try to autofill your password at the same time, rendering the password invalid.

Follow these steps to disable your web browser password *AutoComplete* feature:

Internet Explorer 7/8

- 1) In Internet Explorer, choose **Tools | Internet Options**
- 2) Activate **Content** tab
- 3) In the **AutoComplete** section, click the **Settings** button
- 4) Uncheck the **User names and passwords on forms** check box
- 5) Close both option windows by pressing **OK**

Internet Explorer 6 or older

- 1) In Internet Explorer, choose **Tools | Internet Options**
- 2) Activate **Content** tab
- 3) In the **Personal Information** section, click the **AutoComplete** button
- 4) In the **Use AutoComplete for** group, uncheck the **User names and passwords on forms** check box
- 5) Close both option windows by pressing **OK**

Firefox 2/3

- 1) In Firefox, choose **Tools | Options**
- 2) Activate **Security** tab
- 3) In the **Passwords** section, uncheck the **Remember passwords for sites** check box
- 5) Close options window by pressing **OK**

Opera 9

- 1) In Opera, choose **Tools | Preferences**
- 2) Activate **Wand** tab
- 3) Uncheck the **Let the Wand to remember passwords** check box
- 5) Close preferences window by pressing **OK**

Chrome

- 1) Click the wrench button
- 2) Select **Options**
- 3) Click the **Personal Stuff** tab
- 4) In the **Passwords** section, select **Never save passwords** option
- 5) Click **Close**

Global hot key does not work

There are some global, system wide hot keys that can be configured on “Hot keys tab” under program options. These include *Autofill*, *Autofill password only* and *Activate Password Agent*.

If pressing pre-defined hot key does nothing or another program is activated instead, then your hot key is most probably hijacked by another application. This is possible because these hot keys are system-wide, or global. Only one program can “own” certain hot key combination, while it is running. You may have defined Ctrl+Shift+P hot key combination in *Password Agent*, but when another application uses the same combination and is started before *Password Agent*, system assigns this hot key to another application. Result is that this another application is operated by the hot key, not *Password Agent*.

To solve this problem please review your global hot keys and change them or find out what application uses the same keys and change its configuration accordingly.

Tip: For autofill avoid using global shortcut combination that contains Alt key. Alt key is usually used to access menu commands and keyboard shortcuts and depending on implementation, using Alt key as part of autofill key combination may cause autofill not to work properly in some applications.

Open Link command does not open web pages

Seems you have no default web browser set properly. Try to set your favorite web browser as default browser again.

To set *Internet Explorer* as your default browser:

1. Start *Internet Explorer*, then choose **Tools | Internet Options**
2. Change to **Programs** tab
3. Check “*Internet Explorer should check to see whether it is the default browser*” checkbox
4. Press **OK**

Web links open in the same browser window

By default *Internet Explorer* may open links in an existing browser window, not in a new blank window. If you prefer that the **Entry | Open Link** command should launch your web sites in new browser windows, follow these steps:

1. Start *Internet Explorer*, then choose **Tools | Internet Options**
2. Change to **Advanced** tab
3. In the list, under **Browsing** node unselect **Reuse windows for launching shortcuts** checkbox
4. Press **OK**

Slow or erratic scrolling in entries list

If scrolling entries list is slow or jumpy, you can disable Windows' "smooth-scrolling" feature. This is by default active on Windows XP but unfortunately does not work very well with many applications, including *Password Agent*.

To change this option:

1. Open *System* applet under *Control Panel* by clicking **Start | Settings | Control Panel | System**
2. Switch to **Advanced** tab
3. In *Performance* group, press **Settings** button
4. On *Visual Effects* tab, unselect **Smooth-scroll list boxes**
5. Press **OK**

File is damaged

If you receive message that the file you are trying to open is damaged, you can try to open previous version of the file that *Password Agent* automatically keeps (if you don't have backup of the original file in other folder). Previous versions of the file have extension **.old** plus number, like **.old1**, **.old2** etc. Newest backup file has extension **.old1**, others are older in increasing order. The number of old files available depends on **Count of old files** setting (see "Backup" on page 28) and defaults to 3.

To open previous version of the file:

1. Choose **File | Open**
2. Navigate to the folder where your data file is, so you'll see your file name in the list
3. In *Files of type* combo box, select **Password Agent backup files**, file list will display only backup files with .old+N extensions.
4. Select your file that has **.old1** extension, this is previous version of your damaged file.
5. Press **Open**. If you provide a valid master password, your file will be opened.
6. Save the file with a new name using **File | Save As** command. From now on, use the new file you just saved.

Important: Please note that these .old automatic backup files are missing the latest change you made to your original file. Each time you change your file (add, delete, rename etc), previous version will be saved as .old, and the modified version is saved as the right .pwa file. But *Password Agent* also allows you to keep up to date copy of your data file, see the see "Backup" on page 28 for more information.

Administrator privileges required

In **Windows 2000/XP** administrator privileges are required to enter key code. That way after entering key code the program will be accessible to all users of the

computer. Re-run the program as administrator and try again or ask your system administrator complete the task.

In **Windows Vista/7** with UAC enabled (by default) even if your user account has administrator privileges, programs (like *Password Agent*) that you start will run under limited user account by default. To run *Password Agent* as administrator right-click its shortcut and choose “Start as administrator” command from popup menu. That will start the program as administrator after asking you for confirmation. Now you can enter the key code, after what you can close *Password Agent* and run it again as standard user. If “Start as administrator” command is not available in right-click menu then it is possible that you don’t have administrator rights. On that case ask your system administrator to complete the task.

Knowledge base & forum

For solutions to common problems please see Forum & Knowledge Base area of our internet homepage:

<http://www.moonsoftware.com/forum/>

How to buy

How to Buy

Password Agent is distributed as free limited *Lite* version. See “Lite vs. Unlimited” topic for more information.

To buy unlimited version of *Password Agent* please visit our online store at:

<http://www.moonsoftware.com/store.asp>

You’ll get fully functional *Password Agent* within minutes!

Entering a key code

After purchasing *Password Agent* you will receive a personal key code. You need to enter this key code into *Password Agent Lite* to turn the *Lite* version into the *Unlimited* version. To enter your key code, follow these steps:

1. If you have not yet installed the latest version of *Password Agent Lite*, please do so first. You can download the latest version from our web site [download section](#). **Serial number issued for version 2 will not work in old version 1.**

2. Run *Password Agent Lite*.
3. Choose **Upgrade | Enter Key Code** command. A dialog will open.
4. Type in your name, and serial number exactly the way they appear in the letter you received. **Use the same capitalization, punctuation and spacing as in the e-mail.** You can use copy & paste to ensure the information gets entered correctly.
5. After the information is entered, press the **OK** button. You will see a message that tells if the procedure was successful. If your data was entered correctly, the Upgrade menu will be hidden and your name will be displayed in the **Help | About** box. You are now the registered owner of the program.

Note: It is not possible that a serial number you received from us when purchasing the program is not working. If the program is telling you that your serial number is invalid, first check if you are entering it into the right version of *Password Agent*. That means serial numbers of version 1 of *Password Agent* do not work with version 2 of the program. You need to buy upgrade if you want to use a different version. But if you are sure your program's version is right, then just be sure you enter your name and serial number exactly as it appears in the e-mail. Name is **case sensitive** and must be entered exactly as it appears.

Warning: Print out the entire e-mail that contains your "licensed to" name, serial number and order number for future reference. You will need this information again if you reinstall *Windows*, or want to install *Password Agent* on a different computer. Better safe than sorry.

Uninstalling & Contact Info

Uninstalling Password Agent

Removing *Password Agent* from your system is very easy. This will remove the program files from your hard disk as well as the settings from the registry:

1. Open the *Add/Remove Programs* applet in *Control Panel (Start | Settings | Control Panel)*.
2. Find the *Password Agent* entry in the list and select it.
3. Note step 4 and then close this help file. Otherwise the uninstaller cannot delete it from your system because it is in use.

4. Press the *Remove* button to start removing the application and follow the instructions on the screen.

Contact information

All information about our company, products and services is available on our web site:

<http://www.moonsoftware.com/>

Credits

Special thanks goes to Rob Potter @ Periontech.com and Chris @ eykass.com!

Also, thanks to everyone who has sent us feedback, ideas and bug reports!

Index

A

- Adding a group 9
- Adding a note entry 11
- Adding an account entry 10
- Administrator privileges required 39
- Autofill enters double/invalid password 35, 36
- Autofill feature does not work 34
- Autofill using global shortcut key 27
- Automatically filling login prompts 27

B

- Basic autofill 28

C

- Changing group color 10
- Colors tab 25
- Command Line 32
- Common User IDs tab 26
- Contact information 41
- Creating a new file & setting master password 6
- Credits 41

D

- Deleting a group 9
- Deleting an entry 11
- Description 1

E

- Editing an entry 11
- Entering a key code 40
- Entries 10
- Entry Properties window 11
- Export 33

F

- File is damaged 38

G

- Global hot key does not work 37
- Groups 8

H

- Hiding and reordering columns 20
- Hot keys tab 25
- How secure? 3
- How to Buy 39

I

- Import 32
- Import & export 32

K

- key logger prevention 23
- Keyboard shortcuts 33
- Knowledge base & forum 39

L

- Lite vs. Unlimited 2
- Locking a file 16

M

- Main tab 22
- master password 6
- Moving a group 10
- Moving an entry 11
- Multiple users 26

N

- Network installation 34

O

- Open Link command does not open web pages 37
- Opening a file 14
- Options 22

P

- Password Generator 21
- password input, password edit 23
- prevent keylogger 23
- Printing 18
- Privacy 2

Program layout 7

R

Renaming a group 9

Running Password Agent from removable disk 31

S

Sample workflow using autofill 28

Saving your file 14

Searching 17

Security features 15

Slow or erratic scrolling in entries list 38

Sorting 20

spy program 23

T

TakeWithMe wizard 30

Taking the program with you 30

Templates 29

Templates tab 25

Tips & tricks 26

U

Undo feature 14

Uninstalling Password Agent 41

Useful tools & functions 20

Using expiration date 31

Using QuickSearch 17

Using the Find tool 18

W

Web links open in the same browser window 37